User Manual

GB

cocos-Password Saver

Mobile data security

Your passwords when traveling

cocos-promotions gmbh | talheimer straße 32-d | 74223 flein, germany | phone 0049 (0) 7131/649 38-0 | fax 0049 (0) 7131/649 38-19
www.cocos-promotions.de | www.cocos-promotions.com | www.usb-sticks.de

Content

1 Introduction
2 Software Installation
3 Passwords of the PWS
    3.1 Password
    3.2 Master-Password
4 First Steps
5 The PWS on a PC
    5.1 The PWS-Program
    5.2 Connection
    5.3 Transfer of the Session key
    5.4 Enter Password
    5.5 Managing data sets
        5.5.1 Dialogue for data management
        5.5.2 List of data sets
        5.5.3 Viewing data sets
        5.5.4 Search for data sets
        5.5.5 Enter a new data set
        5.5.6 Automatic Password assignment
        5.5.7 Change data set
        5.5.8 Delete data set
    5.6 Enter Master-Password
    5.7 Changing the Password
    5.8 Changing the Master-Password
    5.9 PWS Settings
    5.10 PWS-Program Settings
    5.11 Data protection
    5.12 Ending the connection
    5.13 Messages of the PWS
6 The PWS mobile
    6.1 Turn the PWS on
    6.2 Icons shown in display
    6.3 Autorepeat
    6.4 Contrast adjustment
    6.5 Enter Password
    6.6 Display of data set
        6.6.1 Choosing initial letters
        6.6.2 Choosing a data set
        6.6.3 Viewing encrypted fields
        6.6.4 Displaying other data sets
    6.7 Turn the PWS off
    6.8 Messages
7 Remarks to Passwords
    7.1 Bad Passwords
    7.2 Good Passwords
    7.3 Handling of Passwords
8 Safety
9 Problems
    9.1 Forgot Password respectively Master-Password
    9.2 PWS disconnected during new encryption
10 Changing the battery
11 Symbol set
12 Legal
    12.1 Exclusion of liability
    12.2 PWS-Program Terms of use
        12.2.1 Use of the program
        12.2.2 Warranty
13 Technical Data

1 Introduction

With your Password Saver (short: PWS) you are able to save passwords and other confidential data securely encrypted. The built-in display allows you to recall them anytime, without depending on a computer.

The PWS offers space for up to 1000 data sets. Each data set consisting of a dialogue field for 32 symbols, which is saved without encryption and a 32 symbol field and two 16 symbol fields, which can be saved encrypted. The dialogue field is used for finding a data set, in the other fields, passwords and other confidential data can be typed-in.

2 Software Installation

Insert the included CD into the CD-ROM drive of your computer. If the Installation-Program does not start automatically, please start the program setup.exe manually from the CD. Then, the software to manage your PWS data will be installed

After successful installation, you can now connect your PWS to the USB-port of your computer. For Windows XP, you will soon be asked for a driver for the PWS. Please give the folder *Drivers* of the CD as the source for it. The necessary drivers will be installed automatically.

If the PWS is not recognized automatically, you will have to install the driver manually (possible for Windows 98). Please use the hardware wizard in the system control for it.

3 Passwords of the PWS

3.1 Password

The password is necessary to recall data saved on your PWS. It has to consist of at least 4 characters, but we strongly recommend to choose a password, which consists of 6 or more characters.

Please enter it on your PC, in order to be able to manage your data from there. You also have to enter it to be able to see your data on the display (see item 6.5).

If the wrong password is entered three times, the PWS will be locked. Then, it won't be possible to enter the password and/or retrieve any data. In order to deactivate the lock you will have to enter the Master-Password on your PC (see item 5.6).

The password can only be changed on a PC (see item 5.7).

3.2 Master-Password

The Master-Password is only necessary to deactivate the lock on your PWS. It has to consist of at least 4 characters, and we also recommend here to choose a longer password. With the Master-Password, no data can be retrieved or decrypted.

If the wrong Master-Password is entered three times in a row, all data on the PWS will be deleted irrevocably. (In case your PWS will ever get lost, you will appreciate this function)

The Master-Password can only be entered at a PC. This is a precaution, so the PWS can not be deleted by accidental "playing".

The Master-Password, too, can only be changed on a PC (see item 5.8).

4 First Steps

Before you can use your PWS, it has to be set up. In order to do so, a password and a Master-Password are needed. Therefore, at first, please think about two good passwords, some tips for it can be found in chapter 7.

Then start the PWS-Program on your PC and connect the PWS with the PC, as described in item 5.2. Afterwards, please transfer the Session key, as described in item 5.3.

The PWS-Program will recognize, that your PWS has not been initiated and the dialog to change the Master-Password will appear automatically. Here, you will have to enter the chosen Master-Password, as described in item 5.8, without having to enter the old Master-Password.

After that, the dialog to change the password will appear. Here, you will have to enter the password, as described in item 5.7. Entering the old password is not necessary here, too.

Setting up your PWS is now completed. The PWS-Program will now show you the input dialog for the password. You can then continue, as described in item 5.4, and save your first data sets on the PWS.

5 The PWS on a PC

5.1 The PWS-Program

The interface of the PWS-Program is divided into several areas, which will be explained shortly. In figure 1 these areas are marked and numbered.

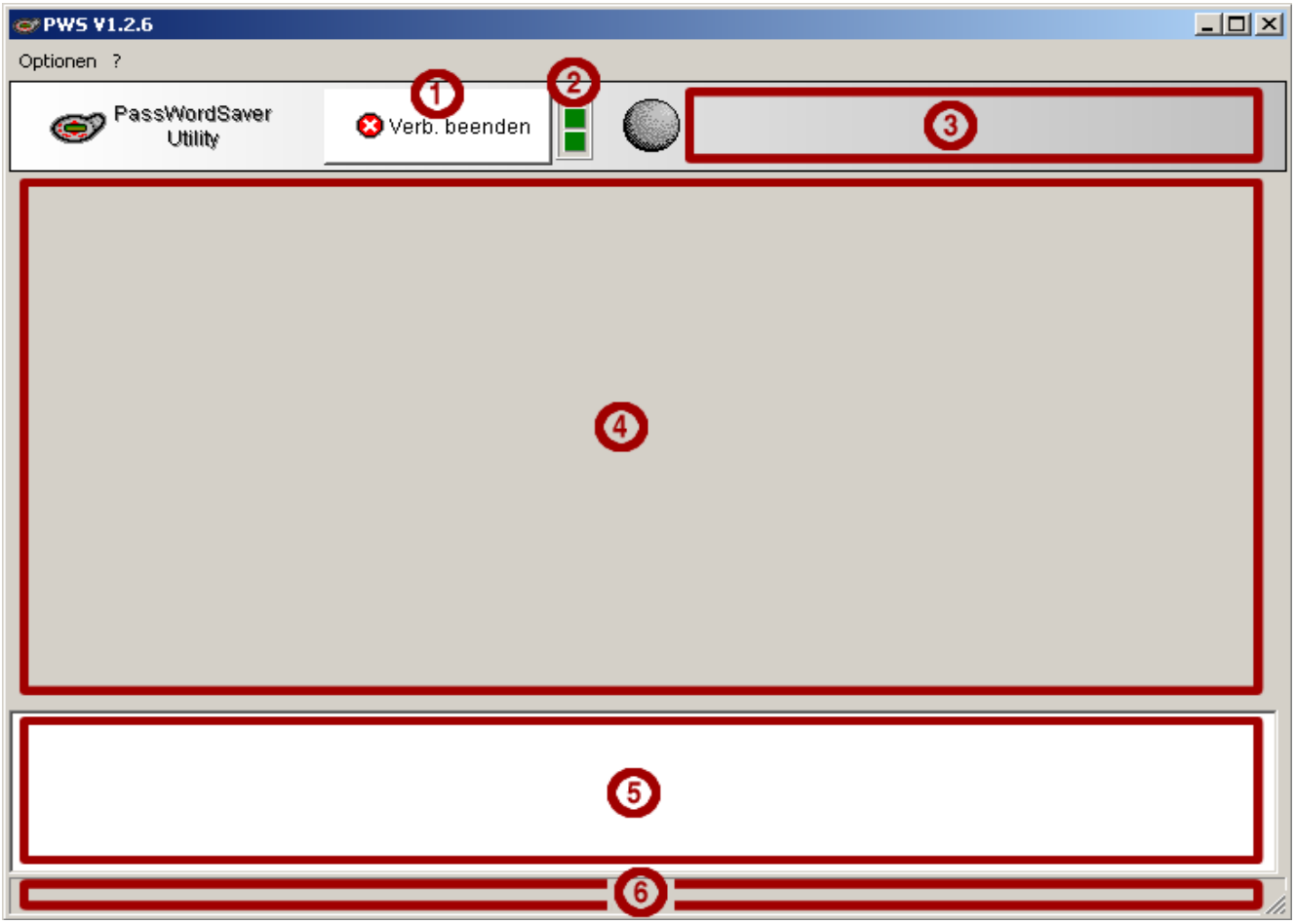

figure 1: Interface of the PWS-Program

1 is the button, with whom you can end the connection with the PWS (see also item 5.12).

2 is there to show, if data is transferred between PWS-Program and PWS. The upper green signal will turn red, if the PWS-Program is sending data to the PWS, the lower one will turn red when receiving data from the PWS.

Even if no activity is performed, the signals will flash shortly about every ten seconds. with it, the PWS-Program will check, if the PWS still can be reached.

3 shows the general status of the PWS. Among other things, you can find out here, if your PWS f.ex. is blocked or was deleted.

4 is the dialog area. Here, different dialogs will appear regarding data management, entering passwords etc.

5 is the message area. Here, all kinds of messages are listed in sequence of their appearance.

6 is the Help-line. Short help texts for all buttons and input fields are displayed.

figure 2
shows a message box of the PWS-Program. Such a message box appears in case of errors or other important incidents. All messages, which appear like that, are also shown in the message area, too.

If you click on [**Message-Boxen nicht mehr anzeigen**], before you close the message, no more message boxes will appear until you start your program again.

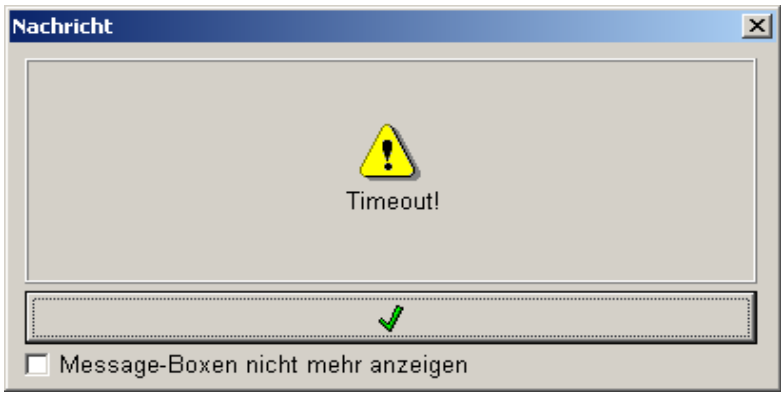

figure 2: Message box of the PWS-Program

The message in figure 2 says, that the PWS-Program has sent a message to the PWS, but after an appropriate period of time, no answer was received yet.

5.2 Connection

In order to connect your PWS and the PWS-Program, you first have to connect your PWS to the USB-interface of your PC and then start the program.

As soon as your PWS is connected to a PC, the message *verbinde ...* will appear in the second line of the display. In figure 3 the start dialog of the PWS-Program can be seen.

figure 3: Start dialog of the PWS-Program

After being started, the program automatically tries to establish a connection to the PWS. If no PWS is connected to the PC, "Bitte schließen Sie einen PWS an ihrem PC an!" and "Kann das Programm nicht starten!" will appear in the message area. (This can also happen, if the drivers were not or not correctly installed.)

You can also establish a connection manually by clicking on the button [**Versuche den PWS zu erreichen**]. This will be necessary, if the PWS is connected after the program was started or if you want to establish a connection again, after the connection was ended.

If the connection establishment was successful, "Hallo von ihrem PWS!" will appear in the message area and the program will change to the dialog for entering the Session key.

5.3 Transfer of the Session key

As soon as PWS and PWS-Program are connected, the PWS will establish a new Session key and this Session key will be displayed in the second row of its display. Now, the dialog for entering the Session key will appear in the PWS-Program (see figure 4).

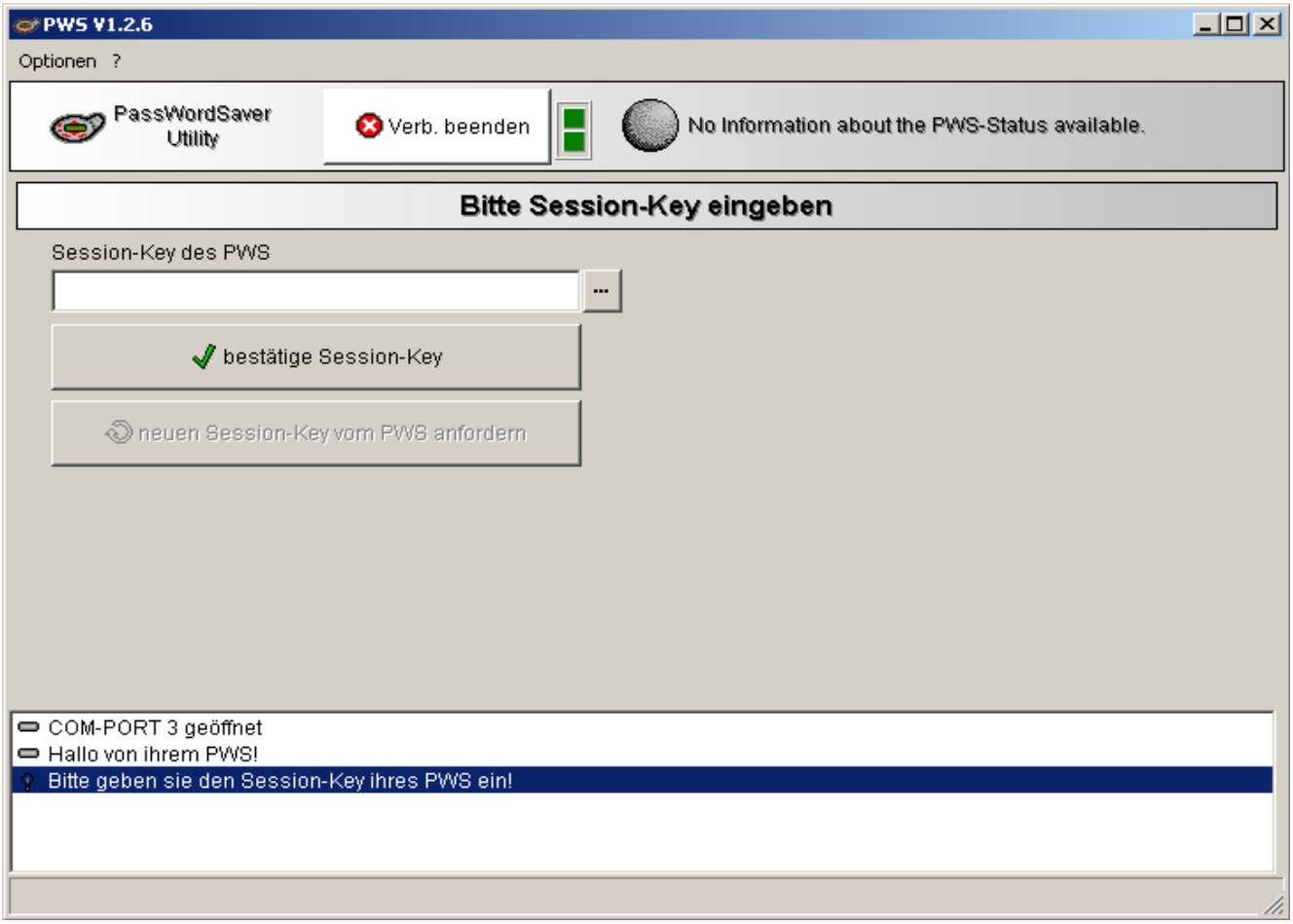

figure 4: Entry of Session key

Here, you have to enter the Session key shown on the PWS. To do so, only the keys of a standard keyboard are required, the Session key will not contain any special, national characters. After clicking on [**bestätige Session-Key**] your entry will be verified.

If there was a wrong entry, "Session-Key-Hash ist ungleich" will appear in the message area. In this case, please click on [**neuen Session-Key vom PWS anfordern**] and repeat the entry. Please not, that a new Session key will be established by the PWS.

If the entry was correct, "Session-Key-Hash ist gleich" will appear in the message area and you will be able to continue.

5.4 Enter Password

After the Session key was transferred, the dialog, shown in figure 5, will appear for the entry of the password. Enter your password and then click on [**bestätige Passwort**].

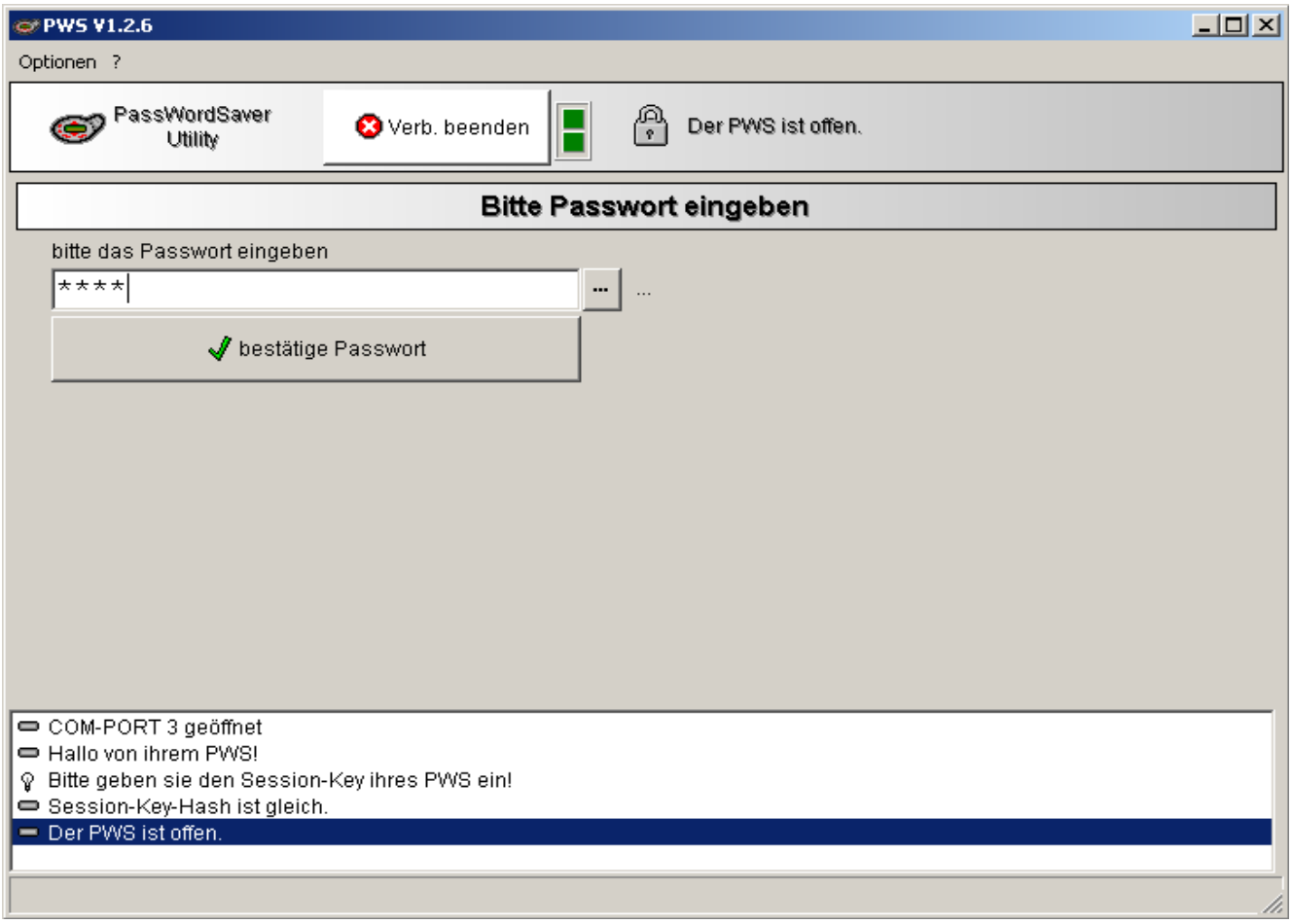

figure 5: Entry of password

The result of the following verification will again be shown in the message area. If your entry was not correct, you can enter your password again. If you enter the wrong password three times in a row, the PWS will be locked. The PWS-Program will notice it and will take you automatically to the dialog for the entry of the Master-Password (see item 5.6).

5.5 Managing data sets

5.5.1 Dialog for data management

figure 6 shows the dialog for the management of data sets. On top, there is a row with icons, with whom, different functions can be selected or buttons can be established. They will be explained below. All functions and buttons can also be opened in the menu.

On the left side, under the row of icons, it is indicated, how many data sets are used in the PWS, respectively how many data sets are still available. Aside, a progress bar appears, when the PWS is busy with a function.

In the area beneath (after requesting it) the list of data sets is shown.

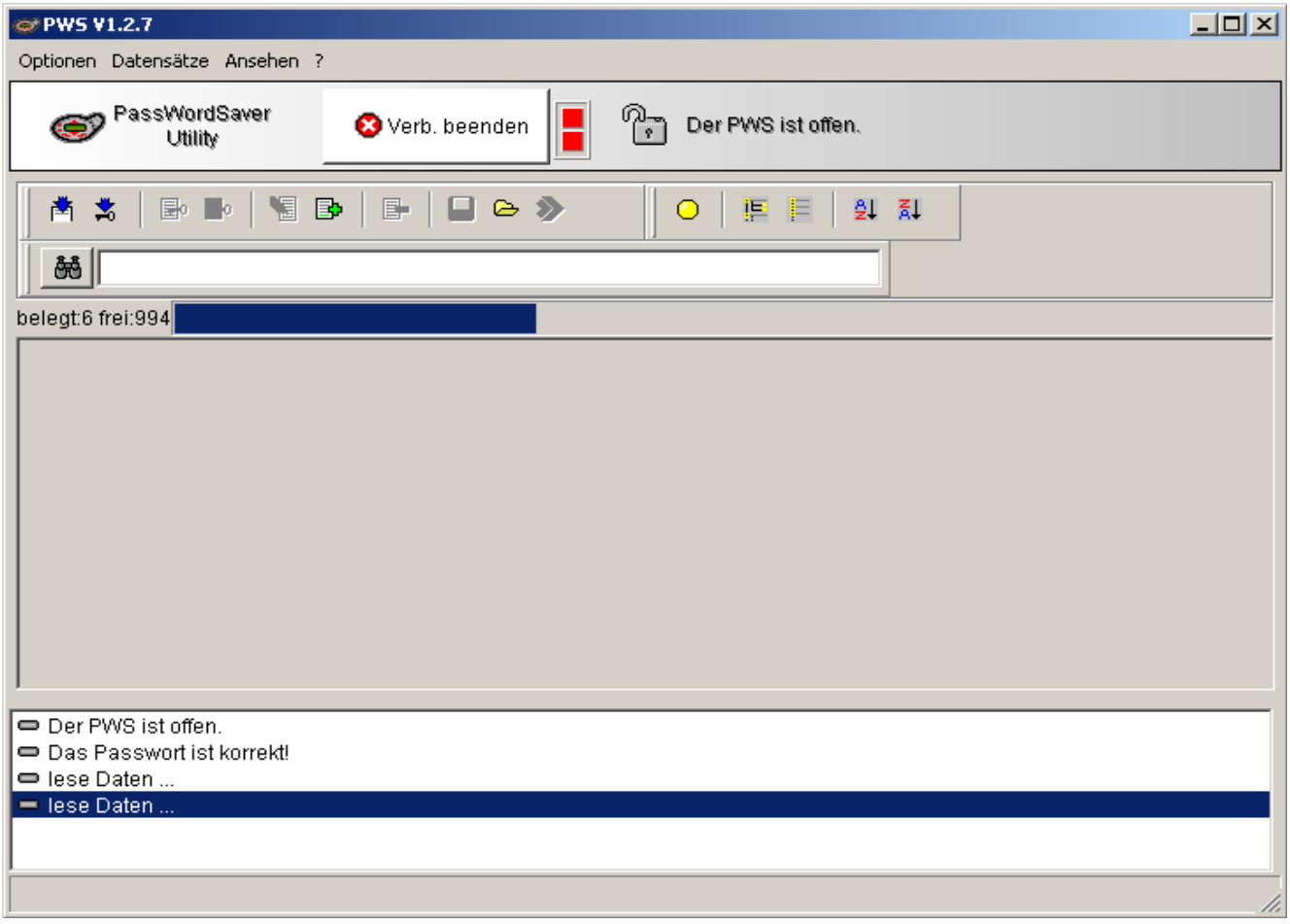

figure 6: Data Management

5.5.2 List of data sets

In order to get the list of data sets, please click on . In doing so, only description and date of the last change, as well as the maximum age of the data set password are displayed, but not the encrypted fields.

In the list then, all descriptions are shown sorted alphabetically in ascending order. With the list can be shown sorted alphabetically in descending order and with again sorted alphabetically in ascending order.

The icons in front of the descriptions have the following meaning:

- The data set is okay.
- The data set password has exceeded the maximum age (see item 5.5.5).
- The encrypted fields were not newly encrypted, when the password was changed, and can no longer be read (see item 5.7).

marks the data set, chosen with a single click.

After clicking on in the icon-row, only data sets, marked with or are shown. When clicking on it one more time, the complete list will be shown again.

5.5.3 Viewing data sets

In order for a data set to be displayed, you will have to open an item in the list with a double click. In doing so, the data set is chosen at the same time. With another double click, it can be closed again. In addition, you can open all data sets with and with , you can close them again. But only date of change and maximum password age of the data set are shown.

With , you are able to receive the encrypted fields of the chosen data set. They will then be decrypted and registered in the list. They will be displayed, when the corresponding item was opened.

With you have the opportunity to receive the encrypted fields of all data sets.

Please consider, that one time retrieved, encrypted fields will be saved in the PWS-Program until you exit this program.

figure 7
shows the dialog for data management with opened list. For the item, listed in the middle, the encrypted fields were already entered, but not for the other ones.

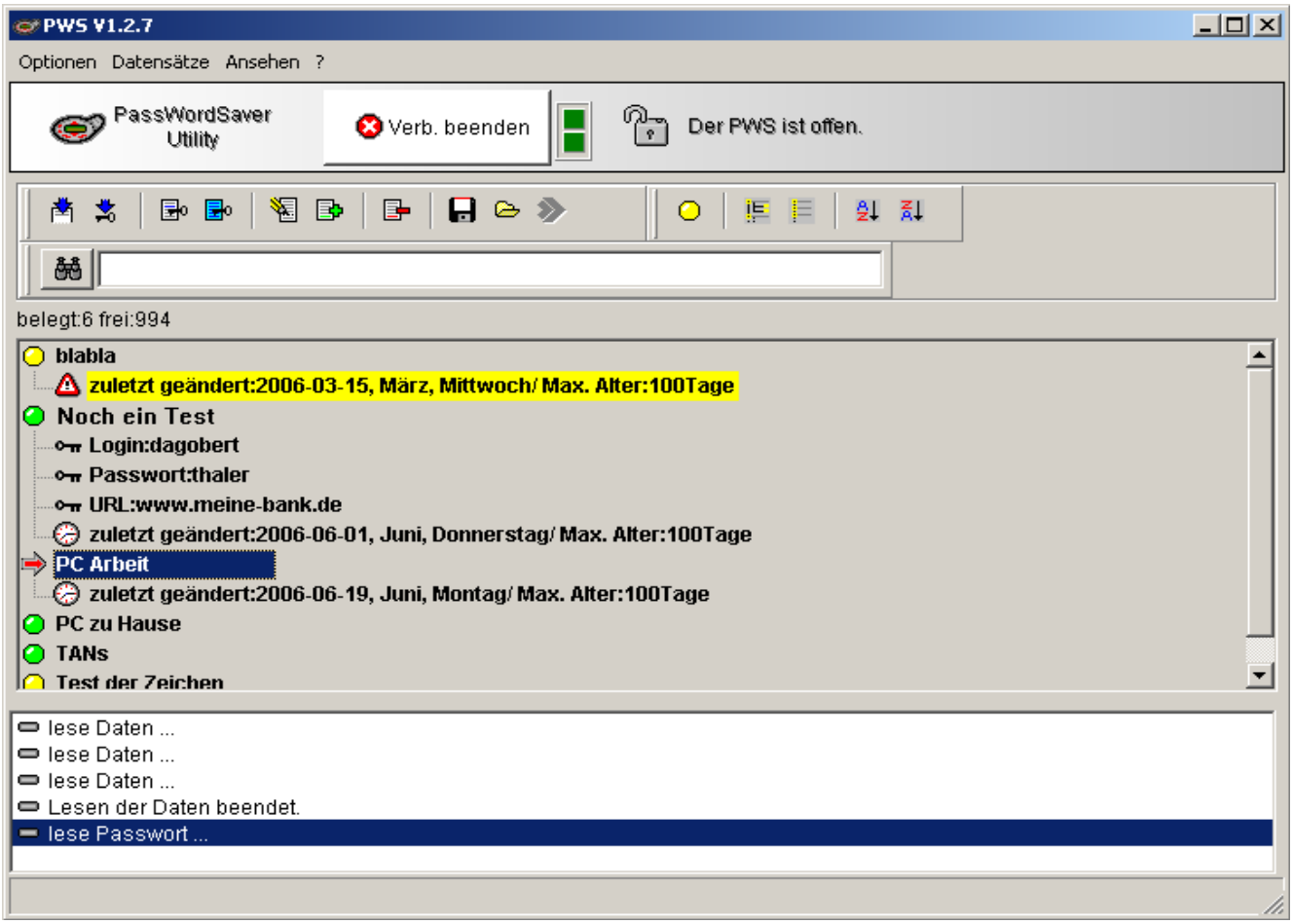

figure 7: Opened list

5.5.4 Search for data sets

With 🔍 and the input field next to it, you can search for data sets. In order to do so, you have to type word (or part of the word) that you are looking for, into the input box and then click on 🔍. The program searches for the first data set, in which the requested word can be found in the description, and then chooses this data set.

With repeated clicks on 🔍 the second, third, etc. data set with the requested word is searched for.

The search only takes place in the descriptions, never in the encrypted fields.

5.5.5 Enter a new data set

With 📝, you are able to create a new data set. After the click, the dialog for the editing data sets will appear (see figure 8).

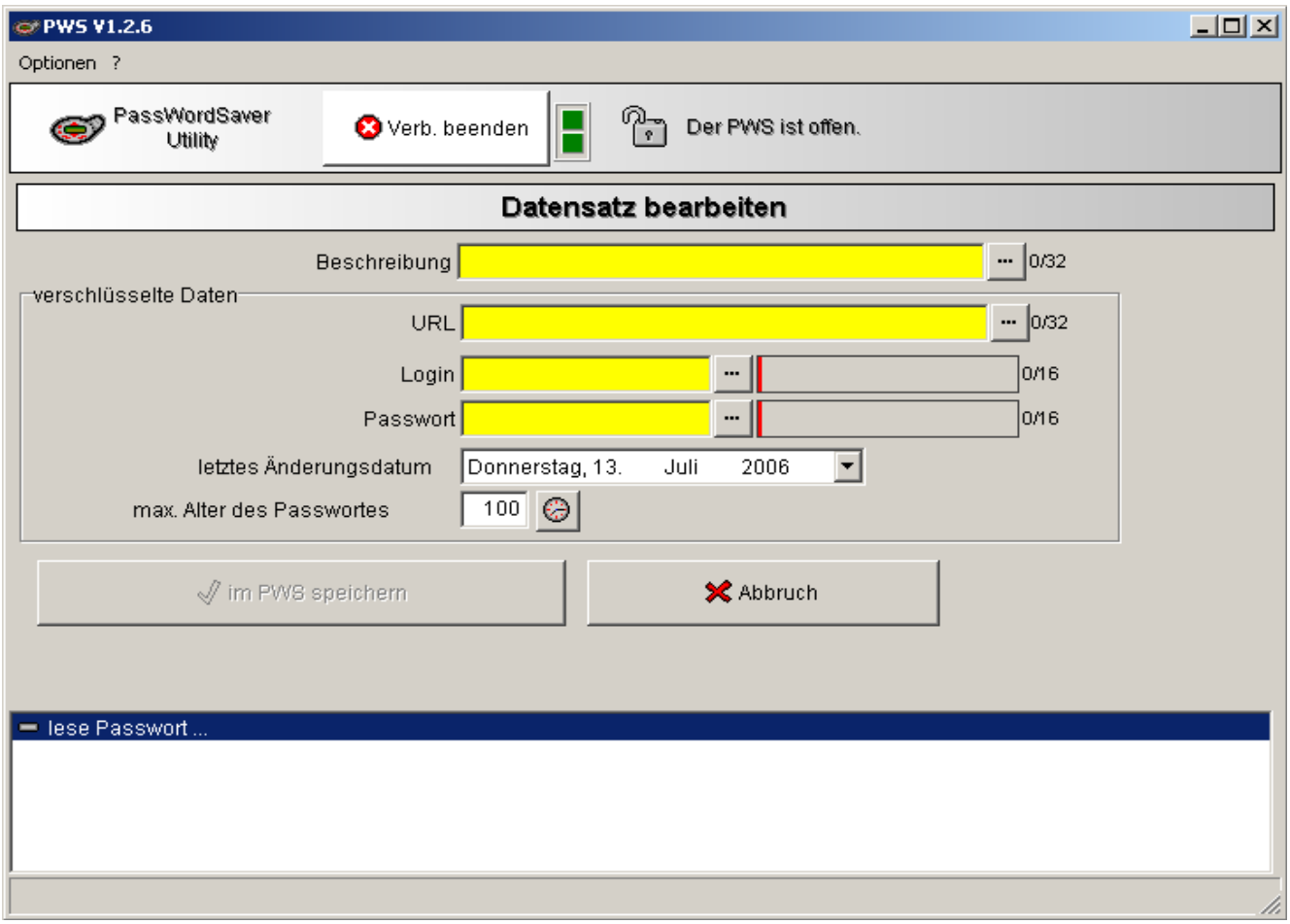

figure 8: Editing data sets

In each one of the fields **Beschreibung** and **URL**, up to 32 characters can be typed in, in the fields **Login** and **Password** up to 16.

The field **letztes Änderungsdatum** always shows the current date.

In **max. Alter des Passwortes** you can enter an age in days, that the password should not exceed. Here, a number between 1 and 9 999 can be entered. If you click on , a select list will appear, with predetermined times like one week, one month, etc.

In case the given time is exceeded, the data set will be marked with . There will be no other consequences. The whole purpose of this function is to remind you to change your passwords on a regular basis.

Only the fields **URL**, **Login** and **Password** will be encrypted.
(According to the name of the field, it is intended, that in the field **URL** the URL of an internet supplier is saved, and in **Login** and **Password** the respective access data is saved. Whatever else you want to save in the encrypted fields is completely up to you.)

The bar next to **Login** and **Password** is supposed to inform you about the quality of your password. The longer the password, and the more different the characters are (small letters, capital letters, numeric characters, phrases and special characters), the longer and darker the bar will become.

Only if the field **Beschreibung** and one of the fields **URL**, **Login** or **Password** are not empty any more, the data set can be saved.

With [**im PWS speichern**] the new data set will be saved in the PWS and the program will the return to the data management dialog. With [**Abbruch**] you will return directly to the data management dialog and the data set then will *not* be saved.

5.5.6 Automatic Password Assignment

On request, you can also receive a random password from the system at any time, which will be transferred directly into the encrypted field **Login** or **Password**. To do so, please click on the button on the right side, next to the rexpective field.

A new window will open up, in which you can determine the length of the password (maximum 16 characters), as well as the nature of the used characters (capital letters – small letters – both, numbers, special characters). Please choose the respective fields for it. When you click on the button with the cube, the password will be generated and, at the same time, transferred into the designated field.

When clicking on the button left side on top, the password will be confirmed and the window will be closed.

5.5.7 Change data set

In order to change a data set, please choose the respective data set and click on . A dialog will appear as seen in figure 8, but here, the input fields are already filled with the current data of the data set you intend to change.

After the data set was changed, it can be saved as described in item 5.5.5.

5.5.8 Delete data set

In order to delete a data set, please choose the respective data set, click on and confirm the following confirmation prompt. The data set then will be deleted in the PWS.

Please consider, that the deletion is irrevocable! There is no possibility to restore a deleted data set, because it will be overwritten in the PWS.

5.6 Enter Master-Password

In case your PWS is locked, you will be asked automatically to enter the Master-Password after entering the Session key, respectively directly after entering a wrong password three times (on the PC).

Here, you have to enter the Master-Password twice, in order to avoid typing errors. Only if both entries are identical, you will be able to send it to the PWS to deactivate the lock.

If you send a wrong Master-Password to the PWS three times in a row, all data in your PWS will be irrevocably deleted! Then, you will have to set up your PWS again, as described in chapter 4.

5.7 Changing the Password

In order to change the password of your PWS, please choose ➔Optionen - neues Passwort in the menu. The dialog, shown in figure 9, will appear.

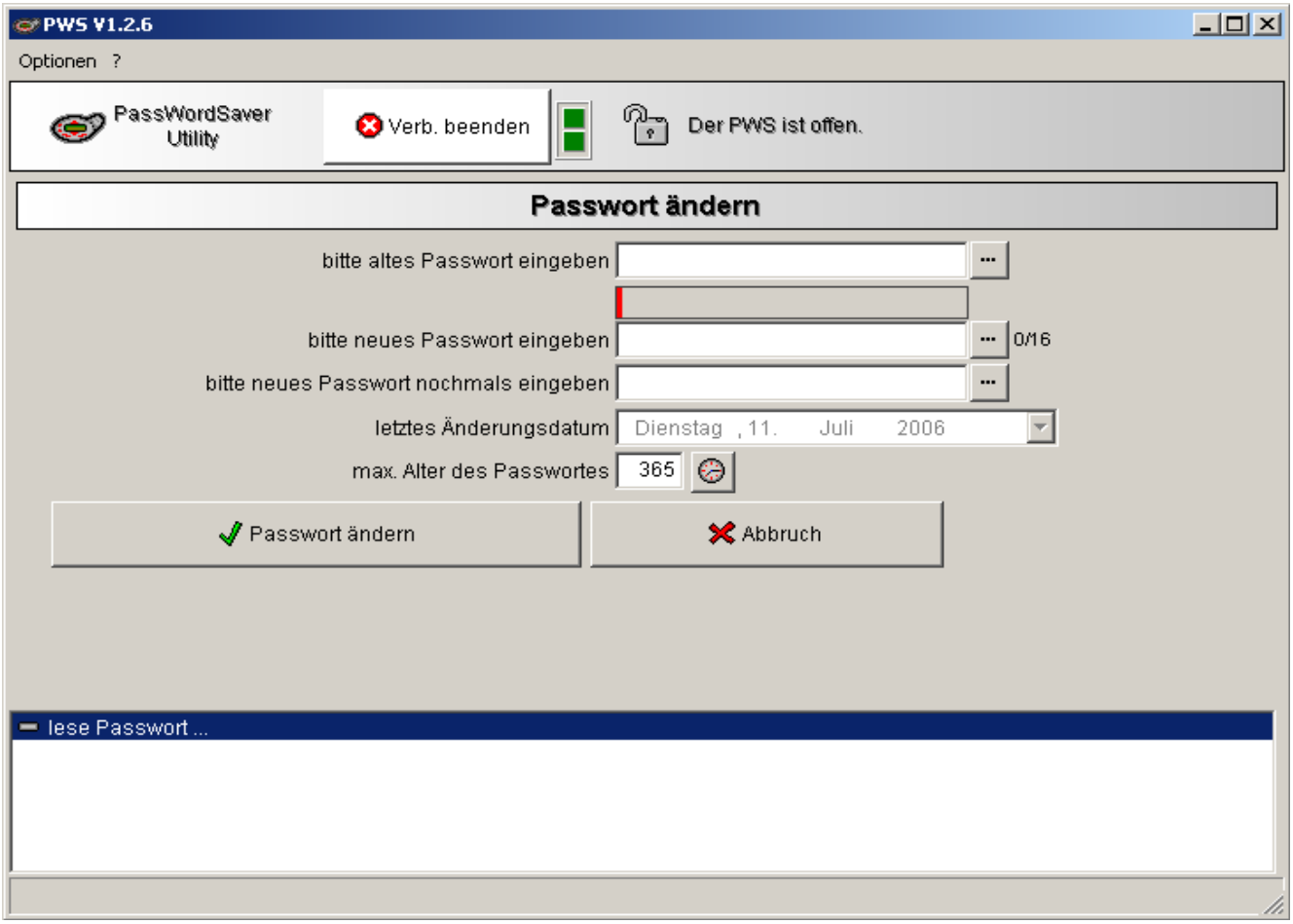

figure 9: Changing the password

In the upper field, you have to enter your old pass word. You then have to enter the new password in each field underneath it. If old and new password have at least four characters, and in both fields for the new password the same characters were entered, then you can save the new password in the PWS with [**Passwort ändern**]. When clicking on [**Abbruch**] you will return to the previous dialog, without changing the password.

The PWS will verify the old password and only save the new password, if the old password was correct. In the message area, the success or failure of the verification will be shown.

As soon as the new password was saved in the PWS, the PWS will start to newly encrypt all data sets. this will take about one minute for 1000 data sets. **During this time, never disconnect the PWS from the USB-interface, in no case! Under unfavourable circumstances, this can lead to loss of data!** With weak batteries, some data sets can be damaged, with empty batteries or without batteries, all data sets, which were not encrypted anew, will therefore not be decipherable anymore.

The new encryption, too, should not be interrupted by ending the connection to the PWS or to the PWS-Program.

During the new encryption, the message *nicht abziehen* will appear on the PWS-display and the PWS-Program will show a progress bar in the data management dialog. After the new encryption ended, *verbunden* will appear in the PWS-display again, the PWS-Program will re-load the list of data sets and, by doing so, will check the success of the new encryption.

the bar over the field **bitte neues Passwort eingeben** is supposed to help you to evaluate the quality of the new password. The longer the password, and the more different the characters are (small letters, capital letters, numeric characters, phrases and special characters), the longer and darker the bar will become.

In addition to the password, its date of change and maximum age will be saved. The date will be set according to the current date. The age is displayed in days and can be within 1 to 9 999 days. When clicking on , you will receive a list with presetting for the maximum age.

5.8 Changing the Master-Password

In order to change the Master-Password, choose ➔Optionen – neues Master-Passwort in the menu. Dialog and operation are the same as in changing the password (see item 5.7), but here, no new encryption will take place after the Master-Password was saved successfully.

5.9 PWS Settings

With the PWS-Program, you are able to change some settings of the PWS. Choose ➔Optionen – PWS-Einstellungen in the menu. A dialog, as shown in figure 10, will appear. Here, you can determine contrast-level of the LCD, length of the Session key, language and keyboard repeat rate of the PWS.

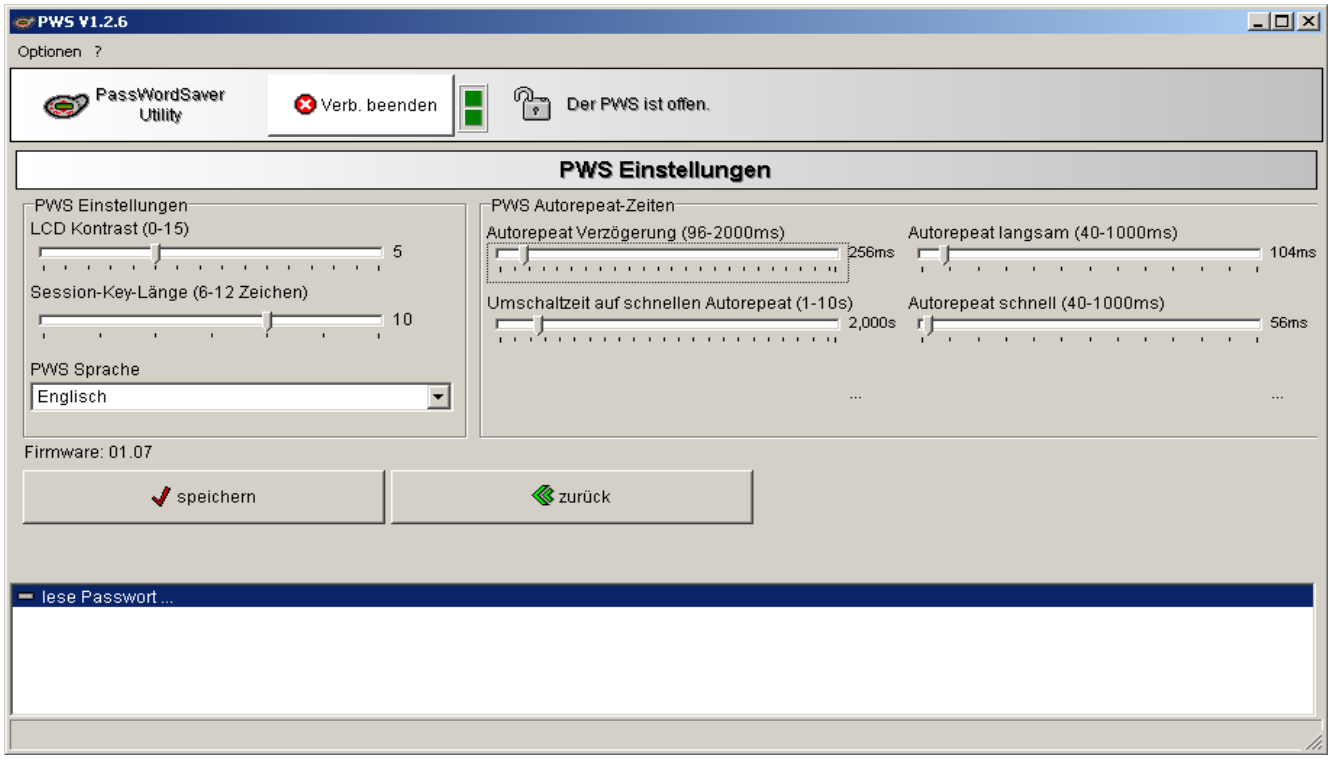

figure 10: PWS-Settings

With [**speichern**] the new settings are saved in the PWS. With [**zurück**] you will return to the previous dialog, not yet saved settings will *not* be written in the process.

A change in contrast will be effective immediately after the setting is saved. A new length of the Session key will not be effective until the next connection is started and a new language will not be effective until a new message appears in the display.

You are able to change the settings several times in a row, in order to obtain the perfect contrast level.

5.10 PWS-Program Settings

Several languages are available for the PWS-Program. In order to choose a language, go to ➔Optionen –Sprache (im Auslieferungszustand ➔Options – Language) in the menu. A dialog box will appear with a list, where you can choose one of the available languages.

The new setting will not be effective until the PWS-Program is started again.

5.11 Data protection

In order to protect all data saved in the PWS, f.ex. to restore them when maybe losing PWS, choose ➔Datensätze – In eine Datei Speichern in the menu. But first, you must have read the passwords of all data sets (Menu ➔Datensätze – Lese Passwörter aller Datensätze), otherwise a respective warning will appear ("Sie haben xx Passwörter nicht ausgelesen").

Choose the desired folder for the data protection and choose a file name for the backup file (f.ex. Protection0605). The file extension (.pws) will be added automatically.

Now, you will be asked to enter a password, consisting of at least 20 letters. Since space characters are also accepted, it is recommended to use a phrase as a password (f.ex. The name of my wife's horse is Rosalinde!).
After entering the password and confirmation with OK, the backup file is created in the chosen folder.

Please copy the backup file onto an external data carrier (Disk, CD or DVD) and delete the file on your computer for safety reasons. The external data carrier should be kept in a safe or some other safe place.

In order to retrocede all data onto your PWS , choose ➔Datensätze – Aus einer Datei laden in the menu.

If you do not want to copy the data of the backup file into a new (empty) PWS, instead you want to transfer the changed data of the backup file onto the PWS (f.ex. you rotational receive a new backup file with new access data for certain areas of your company from your system administrator and you want to save them on your PWS), you first must have read the passwords of all data sets in the PWS, too (Menu ➔Datensätze – Lese Passwörter aller Datensätze), otherwise, a respective warning will appear ("Sie haben xx Passwörter nicht ausgelesen").

When transferring data from the backup file onto the PWS, then please also be careful not to overwrite your current data in the PWS with older data from your backup file. The indication on the right side of the data sets in your backup file will inform you, which data sets are not placed in the PWS, or have a different age or password. The question mark (?) will remind you, that the passwords of these data sets have not been read in the PWS (in order to correct it: Menu ➔Datensätze – Lese Passwörter aller Datensätze).

Via double click, single data sets can be chosen to be transferred to the PWS (*x* - will appear on the right side of the chosen data set).

5.12 Ending the connection

With the button [**Verb. beenden**] you are able to end the connection to the PWS at any time. The program then will change to the initial dialog (figure 3) and the PWS will display *Verbindung beendet*.

The message on the PWS will be shown for 10 seconds. During this time no new connection can be established. After that, *verbinde* ...will appear in the display again.

Never end the connection during the process of the new encryption!

The connection ends automatically, when the communication between PWS and Program is disturbed by too many transmission errors. Reasons for this could be f.ex. a damaged USB-cable or USB-hub, or other defective programs.

In case the PWS is disconnected from the USB-interface without correct, previous software log-off the program will realize this after a few seconds and will then end the connection. **However, you should never end the connection through unplugging, because under unfavourable circumstances (f.ex. when a data set is written right this minute) this can lead to loss of data!**
If the PWS-Program is ended, it will automatically end any still existing connection.

5.13 Messages of the PWS

Listed below are the messages, that can appear during operation on a PC:

verbinde ...
Appears, as soon as the PWS is connected to the USB-interface of your PC. The keys of the PWS are now deactivated, that means, the PWS can only be operated via PC. While this message can be seen on the display, the PWS can be disconnected riskless from the USB-interface.

Schlüssel:
XXXXXXXXXX
Appears, after a connection was established. Instead of *XXXXXXXXXX*, the Session key of this connection is shown in the second row.

verbunden
Appears, after verification of the Session key, no matter if it was successful or not. (Only the PWS-Program can decide, if the verification of the Session key was successful.)

Verbindung
beendet
Appears, after the connection was canceled with [**Verb. beenden**] or because of several transmission errors. The PWS can now be unplugged riskless, unless you interrupted the connection during a new encryption. This message will remain on the display for ten seconds. After that, *verbinde ...* will appear again.

Verbindung
Spion?
Appears 10 seconds before *Verbindung beendet* will appear, in case a transmission error has occurred, which leads to the conclusion, that a malicious program has tried to take over the connection to the PWS.

! nicht !
! abziehen !
Appears during the new encryption of the data sets after the password was changed. Unplugging the PWS while this message is visibleon the display, can now lead to a loss of data.

6 The PWS mobile

6.1 Turn the PWS on

In order to turn the PWS on, please first press the button ↵ and then the button ⏻ in addition. Hold both buttons for about three seconds. (Since two buttons have to be pressed to turn the device on, it is avoided that the device is turned on accidentally.) After that, the text *Password Saver* will appear on the display. Now, the PWS is turned on.

As soon as you release the buttons, *weiter Enter* will appear on the display. With ↵, you will reach the password entry and with ◀, the contrast settings.

Instead of *weiter Enter*, some other messages can appear. These are described under item 6.8.

6.2 Icons shown in display

On the right side of the display, five icons can appear, ◀ and ▶ (top), as well as ▲ and ▼ (bottom). In the middle, there is the icon .

When data set descriptions or encrypted fields are displayed, the icons ◀ and ▶ are used in the following ways:

Icon	Meaning
	The displayed text size does not exceed 12 characters and is shown completely.
▶	The displayed text has more than 12 characters and the beginning is displayed. Scrolling is possible with ▶.
◀	The displayed text has more than 12 characters and the end is displayed. Scrolling is possible with ◀.
◀ ▶	The displayed text has more than 12 characters and neither beginning nor end are displayed. In this case, scrolling is possible with ◀ and ▶.

While browsing through the listed data set descriptions and encrypted fields of a data set, the icons ▲ and ▼ are used in the following ways:

Icon	Meaning
	The list has only one item. This one item is displayed.
▼	The list has a minimum of two items and the first one is displayed. With ▼, changing to the next item is possible.
▲	The list has a minimum or two items and the last one is displayed. With ▲, changing to the previous item is possible.
▲ ▼	The list has more than two items. With ▲ and ▼, browsing through the list is possible.

If appears in the display, the battery of your PWS is empty and has to be changed (see chapter 10).

6.3 Autorepeat

The keys of the PWS have an Autorepeat function, that means, if one button is pressed for a longer time, the PWS is acting as if you would have pressed the button several times in a row.

First, the repeat rate is about 5 icons per second, after about three seconds, it goes up to about 10 icons per second.

6.4 Contrast adjustment

If the characters can hardly be seen, then you will have to adjust the contrast. To do so, please press the button ◀, while the message or the text *weiter Enter* appears on the display.

In the first row of the display, *Kontrast* is now shown, and in the second row, the bar with the current setting is shown.

With ▲, you can now increase the contrast and with▼, you can decrease it. When adjusting the contrast is completed, you can go back with ↵, that means either to *weiter Enter* or the last message will be repeated.

6.5 Enter Passwort

If you press the button ↵ while the message *weiter Enter* is visible on the display, you will reach the password entry. In the first row, *Passwort* will appear, and the second row will be filled with block characters.

These block characters are not valid for a password. Only the characters previous to the first block character are used for the password, that means, the sign you currently edit, will always be the last sign of your entry.

With ▲ and ▼, you are able to change a character of the password. With ▼, you can go forward in the list of all possible characters (see chapter 11), f.ex. from A to B, and with ▲, you can go backwards.

With ▶, you can go to the next character, and with ◀, you can change already typed characters again. In doing so, the characters on the right side are replaced again by block characters. With ▶, you then have to go back to the last character of your password, and in doing so, the already typed characters will appear again.

The password entry is ended with ↵. the password then is checked by the PWS. If it has less than 4 characters, you will receive the message *zu kurz!* (see item 6.8) in the second row. If you entered the wrong password, then you will receive the message *falsch!*. In both cases, you are able to correct the entered password after the message.

If the correct password was entered, then you will automatically go to the choice of initial letters (see item 6.6.1).

Please note, that after successful entry of the password until the PWS is turned off, all data saved in your PWS will be visible unencrypted.

6.6 Display of data set

6.6.1 Choosing initial letters

After successful entry of your password, *Buchstabe* will appear in the first row, followed by an *A*. With ▲ and ▼, you are now able to choose an initial letter. Possible are A-Z with small or capital letters, 0-9 or a * for all other initial characters.

With ↵ , you will go to the options of descriptions. If no data sets are available with the chosen initial letter, the message *keine Daten!* will appear in the second row (also see item 6.8). After the message appeared, you are able to enter another letter.

6.6.2 Choosing a data set

After you chose an initial letter, *Beschreibung* will appear in the first row. In the second row, the description of the first data set with this initial letter will appear.

With ▲ and ▼, you can browse the list of descriptions. If you reach f.ex. with ▼ the end of the list and you operate this button again, you will automatically go back to the beginning of the list. The same applies for ▲.

With the buttons ◄ and ► you are able to scroll description texts with more than 12 characters horizontally.

If you found the desired data set, you are able to have its encrypted fields displayed with ↵.

6.6.3 Viewing encrypted fields

After you chose a data set, its description appears in the first row. The three encrypted fields are now shown decrypted and the content of the first, not empty field is shown in the second row.

With ▲ and ▼, you are able to change between the fields. If you f.ex. reach the last field with ▼ and you press this button one more time, then you will automatically go to the first field again.

If the content of one field is longer than 12 characters, then you are able to horizontally scroll with ◄ and ►.

With ↵ you can return to the choice of initial letters.

6.6.4 Displaying other data sets

After viewing the encrypted fields of a data set, you can return to the choice of initial letters with ↵. There, the last chosen letter will already be preselected.

If you do not choose another letter, and just press ↵ one more time, then the selection of data sets with the last chosen letter will begin. In doing so, you are able to view two data sets back-to-back fast.

6.7 Turn the PWS off

With ⏻, you can turn the PWS off at any time.

If you do not press a button for about one minute, then the PWS will be turned off automatically.

After the device is turned on again, the password has to be entered again.

6.8 Messages

Below, all messages are listed, that can appear, while being operated with a battery. It is possible to abort messages, which appear for ten seconds, with ▶, too. In addition, the contrast can be adjusted while such a message appears, as described in item 6.4.

PassWord
Saver
Appears, as soon as the PWS is turned on and is replaced by another message, as soon as the buttons and are released (see item 6.1).

call
supplier
An error has occurred. In this case, please contact the manufacturer. The message appears for ten seconds, then the PWS is turned off automatically again.

new PWS
init with PC
Appears, after the PWS is turned on, when the PWS has not been set up yet, as described in chapter 4. The message is visible for ten seconds, then the PWS is turned off automatically again.

PWS
data erased
Appears , after the PWS is turned on, in case the PWS was erased after the wrong Master-Password was entered three times. The message is visible for ten seconds, the PWS is turned off automatically again.

PWS
gesperrt !
Appearts, after the PWS is turned on, or after the message *Passwort falsch!*, if the PWS was locked after entering the wrong password three times. The message is visible for ten seconds, the PWS is turned off automatically again.

Neuverschl.
bitte zum PC
Appears, after the PWS is turned on, if the PWS was unplugged from the USB-interface during a new encryption. The PWS can not be used mobile again, until the new encryption was completed (see item 5.7 and item 9.2). The message is visible for ten seconds, the PWS is turned off automatically again.

PWS
weiter Enter
Appears, after the PWS is turned on, when everything is alright.

Passwort:
zu kurz!
Appears, if less than 4 characters of the password were entered, before the button was pressed. After ten seconds, you can continue with the entry.

Passwort:
falsch !
Appears, if the entered password was wrong. If it was the first or second failed attempt, then the entry can be corrected after ten seconds. If it was the third failed attempt, then the message *PWS gesperrt!* will appear after ten seconds.

PWS
leer !
Appears after selecting an initial letter if the PWS contains no data sets. The message is visible for ten seconds, then the PWS is turned off automatically again.

Buchstabe: ?
keine Daten !
Apppears, if there is no data set, whose description starts with the chosen letter. After ten seconds, another letter can be selected. Instead of *?*, the chosen letter will be visible.

7 Remarks to Passwords

7.1 Bad Passwords

A listing of bad passwords can probably be found on your bookshelf, too. This list is commonly called a dictionary. Put in another way, that means: Words, that can be found in a dictionary are bad passwords.

The same is true for names, no matter if names of people, animals or fictitious characters are chosen. Unsuitable passwords, too, are terms regarding work or hobby.

And please, do consider, that words from your personal surrounding can be relatively easy figured out by others.

Even letter combinations, which basically do not make any sense, can be bad passwords. Combinations, which make a pattern on a keyboard (f.ex. rfvbhu or nhuikm), are relatively easy to recognize, when looking over your shoulder.

The same is true for numbers, like f.ex. birthdays, account- or telephone numbers. They are unsuitable for passwords. Another reason, why numbers should not be used as passwords is, that numbers only have a relatively small amount of possible combinations, f.ex. 6 digits only add up to 1,000,000 possible combinations, while 6 small letters already add up to 308,915,776 different combinations.

7.2 Good Passwords

Good passwords have small letters, capital letters, digits, punctuation marks and special characters. The larger the reserve of characters, that can be used for passwords, the better it is.

When keeping some basics in mind, good passwords are relatively easy to find. The more random characters are used for passwords, the better it is. Whoever would like to have a completely random password, can create one by playing dice. In order to do so, each possible character for a password will be assigned with its own combination out of three dice digits. Then, you roll the dice three times and the character with the received combination will be chosen. In case there is no character for the received combination, then simply roll the dice again to receive another combination.

One problem of good passwords is, that they usually are hard to remember. Whoever can not remember passwords like M3yoDfa+mN (it should be clear, that this password can not be used, since it was mentioned here), can create a password out of initial letters and ending letters of words from a sentence (One can also always use the second or third etc. letter of a word. Or one uses the initial letter of the first word, the second letter of the second word, etc.). There is no need to create a sentence, which reflects reality. Yet, the sentence should include numbers, that will also appear as numbers in the password. In addition, certain words can be replaced by special characters. The above mentioned password f.ex. was created out of the sentence "My three year old daughter fools around and makes nonsense.". If you take the ending letter and write some capital letters, then the above mentioned sentence would create the password Y3rdRsd+sE.

7.3 Handling of Passwords

Passwords should be remembered and not written down. In case, somebody absolutely wants to write down a password, then this note should be kept in a safe place, like f.ex. a safe or a safe-deposit box. Places like under a computer, monitor or keyboard, in a computer or battery compartment of the PWS are no safe places!

To save passwords in a text file on a PC is also very careless. An incorrect configuration of the PC is enough to expose such a file in the entire internet. Some computer viruses and worms are even specifically looking for passwords and access data on an infected PC.

Of course, everybody knows not to write down the password of the PWS on its back side or to stick a note to the computer monitor with the password on it.

Also, a password should only be used one time. That means, that each device, secured with a password (computer, PWS, PDA etc.), and each service, secured with a password (Free-Mail, forums etc.) will receive its own password. Since you will only have to remember the password of the PWS in the future, this no longer should be a problem to you.

Passwords also should be changed on a regular basis. In doing so, a new password should be used every time, because it is not safe to use old passwords again (maybe the old passwords were spied out during the last virus attack).

When entering a password, you should make sure that nobody watches you over your shoulder. And please, never look somebody else over the shoulder, when this person is entering a password.

Apart from only a few exemptions, you should never pass on your password. (one exemption f.ex. could be your company laptop, whose password you can give to your boss, so all data on it is available, when you are sick, f.ex.) this is especially true for the password of your PWS, because this gives access to all of your other passwords.

8 Safety

Here are some notes regarding the safety of your PWS:

- As encryption algorithm, AES 128 in the CBC-mode is used. This is standard, and as such tested very good and so far unbroken.
- The key for AES is generated out of the password. This means, that the effective length of the key depends on the password (see item 5.7). It will always be smaller than 128 Bit.
- Neither Master-Password, password nor the key, generated out of it, are saved in the PWS.
- From password and Master-Password, only their hash value is saved in the PWS. A hash-function is a one-way function, meaning, that it is almost impossible to determine password, respectively Master-Password from it. (a so-called Brute-Force-Attack is always possible, but requires a lot of computing power, because with it, all possible passwords have to be tried. A PC, conforming with today's state of technology, would need over 100 years of calculating time, if it has a good password (please compare item 7.2).)
- The PWS will only release all saved data, when it received the right hash value of the password.
- Before transferring the (Master-)password hash value to the PWS, it will be encrypted with the Session-Key. So it is not possible to catch the hash value and send it again later, in order to force the PWS to release all saved data.
- The Session-Key is created with a Pseudo-Random Number-Generator, which additionally also uses the point in time of single keypresses. The quality of the random numbers will be even better, if the PWS is used mobile on a regular basis.
- When a data set is deleted, it will be overwritten completely and not only marked as being free.
- The encrypted fields will also be saved in encrypted form in the PWS and will only be transferred to a PC in encrypted form.

- When the wrong password was entered three times, the PWS will be locked (see item 3.1).
- After the wrong Master-Password was entered three times, the PWS will be erased (see item 3.2).
- The Firmware of the PWS can not be changed. Therefore, no Firmware can be installed, which allows a spying on the PWS.
- The PWS-Program will overwrite its data, when it is ended.

9 Problems

9.1 Forgot Password respectively Master-Password

In case you forgot the normal password, you can try it three times, before the PWS is locked.

In case you forgot the Master-Password and the PWS was already locked, you can try it three times, before all data will be erased.

The manufacturer can not help you in this case. Because if a method would exist, justifiable by costs and/or time, to reconstruct the data saved in your PWS, then the PWS would not be safe anymore.
.

Important note:
Data saved in the PWS can only and exclusively be decrypted with the password! Decryption with the Master-Password is not possible. The Master-Password is only there to unlock the PWS.

Explanation:
Since all data is encrypted with the password (and not with the Master-Password), this data can only be decrypted with this password. If the data could be decrypted with the Master-Password, then the key would have to be placed in the PWS and that would not help data security at all. You could compare this to a spare key under the doormat.

9.2 PWS disconnected during new encryption

Plug the PWS again into the USB-interface of the (running) PC. it is not necessary, that the PWS-Software is running on this PC.

On the display of the PWS the warning message *nicht abziehen* should appear again. That means, the PWS will continue with the new encryption. Only unplug the PWS, if *verbinde ...* appears on the display.

This is only possible, if the battery of your PWS are not empty. But even with a full battery, you might have lost some data sets, which means that they can not be read anymore, respectively can not be decrypted anymore.

10 Changing the battery

In order to be able to find passwords, saved in the PWS, without a PC, the PWS needs a battery. The battery was already inserted in the factory. It is only needed for mobile operation, your data is saved even without a battery.

figure 11: PWS with inserted battery

The battery has to be changed, when the icon appears in the display. But this icon only appears, if the PWS is turned on and not connected to a PC.

figure 12: PWS with applied cover

In order to change the battery, please open the battery compartment on the bottom side of the PWS, by turning the cover approx. 45° anti-clockwise (f.ex. with a coin). Take the old battery out and insert the new one at an angle, with the positive pole (+) towards the front. Please make sure, that the battery is located under the hooks (see figure 11).

Close the battery compartment again by applying the cover, as seen on figure 12 , and pushing it down. Then turn the cover approx. 45° clockwise to firmly close the battery compartment.

A lithium battery, type CR2032, is used. Spare batteries can be bought f.ex. at your local computer store.

11 Character set

Internally, the PWS uses the ANSI character set. The following table shows this one. The columns feature the character and its value as a hexadecimal notation (Hex).

In the column SK those characters are marked, who are used for the Session key, and in the column PW, all characters are marked, which can be used for the password.

Zeichen = character

Zeichen	Hex	LCD	SK	PW
	0x20			×
!	0x21	!		×
"	0x22	"		×
#	0x23	#		×
$	0x24	$		×
%	0x25	%		×
&	0x26	&		×
’	0x27	’		×
(	0x28	(		×
)	0x29	)		×
*	0x2A	*		×
+	0x2B	+	×	×
,	0x2C	,		×
-	0x2D	-	×	×
.	0x2E	.		×
/	0x2F	/		×
0	0x30	0	×	×
1	0x31	1	×	×
2	0x32	2	×	×
3	0x33	3	×	×
4	0x34	4	×	×
5	0x35	5	×	×
6	0x36	6	×	×
7	0x37	7	×	×
8	0x38	8	×	×
9	0x39	9	×	×
:	0x3A	:		×
;	0x3B	;		×
<	0x3C	<		×
=	0x3D	=		×
>	0x3E	>		×

Zeichen	Hex	LCD	SK	PW
?	0x3F	?		×
@	0x40	@		×
A	0x41	A	×	×
B	0x42	B	×	×
C	0x43	C	×	×
D	0x44	D	×	×
E	0x45	E	×	×
F	0x46	F	×	×
G	0x47	G	×	×
H	0x48	H	×	×
I	0x49	I	×	×
J	0x4A	J	×	×
K	0x4B	K	×	×
L	0x4C	L	×	×
M	0x4D	M	×	×
N	0x4E	N	×	×
O	0x4F	O	×	×
P	0x50	P	×	×
Q	0x51	Q	×	×
R	0x52	R	×	×
S	0x53	S	×	×
T	0x54	T	×	×
U	0x55	U	×	×
V	0x56	V	×	×
W	0x57	W	×	×
X	0x58	X	×	×
Y	0x59	Y	×	×
Z	0x5A	Z	×	×
[	0x5B	[		×
\	0x5C	\		×
]	0x5D	]		×
^	0x5E	^		×
_	0x5F	_		×
‘	0x60	`		×

Zeichen	Hex	LCD	SK	PW
a	0x61	a	×	×
b	0x62	b	×	×
c	0x63	c	×	×
d	0x64	d	×	×
e	0x65	e	×	×
f	0x66	f	×	×
g	0x67	g	×	×
h	0x68	h	×	×
i	0x69	i	×	×
j	0x6A	j	×	×
k	0x6B	k	×	×
l	0x6C	l	×	×
m	0x6D	m	×	×
n	0x6E	n	×	×
o	0x6F	o	×	×
p	0x70	p	×	×
q	0x71	q	×	×
r	0x72	r	×	×
s	0x73	s	×	×
t	0x74	t	×	×
u	0x75	u	×	×
v	0x76	v	×	×
w	0x77	w	×	×
x	0x78	x	×	×
y	0x79	y	×	×
z	0x7A	z	×	×
{	0x7B	{		×
|	0x7C	|		×
}	0x7D	}		×
~	0x7E	~		×
	0x7F			
€	0x80	€		×
	0x81			
‚	0x82	‚		

Zeichen	Hex	LCD	SK	PW
f	0x83	*f*		
„	0x84	„		
. . .	0x85	...		
†	0x86	†		×
‡	0x87	‡		×
ˆ	0x88	ˆ		
‰	0x89	‰		×
Š	0x8A	Š		×
‹	0x8B	‹		×
Œ	0x8C	Œ		×
	0x8D			
Ž	0x8E	Ž		×
	0x8F			
	0x90			
‘	0x91	‘		
’	0x92	’		
“	0x93	“		
”	0x94	”		
•	0x95	•		
–	0x96	-		
—	0x97	–		
˜	0x98	˜		
™	0x99	™		
š	0x9A	š		×
›	0x9B	›		×
œ	0x9C	œ		×
	0x9D			
ž	0x9E	ž		×
Ÿ	0x9F	Ÿ		×
	0xA0			
¡	0xA1	¡		×
¢	0xA2	¢		×
£	0xA3	£		×
¤	0xA4	¤		×

Zeichen	Hex	LCD	SK	PW
¥	0xA5			×
¦	0xA6			
§	0xA7			×
¨	0xA8			
©	0xA9			
ª	0xAA			
«	0xAB			×
¬	0xAC			×
-	0xAD			
®	0xAE			
¯	0xAF			
°	0xB0			×
±	0xB1			×
²	0xB2			×
³	0xB3			×
´	0xB4			
µ	0xB5			×
¶	0xB6			
·	0xB7			×
¸	0xB8			
¹	0xB9			×
º	0xBA			
»	0xBB			×
¼	0xBC			×
½	0xBD			×
¾	0xBE			×
¿	0xBF			×
À	0xC0			×
Á	0xC1			×
Â	0xC2			×
Ã	0xC3			×
Ä	0xC4			×
Å	0xC5			×
Æ	0xC6			×

Zeichen	Hex	LCD	SK	PW
Ç	0xC7			×
È	0xC8			×
É	0xC9			×
Ê	0xCA			×
Ë	0xCB			×
Ì	0xCC			×
Í	0xCD			×
Î	0xCE			×
Ï	0xCF			×
Ð	0xD0			×
Ñ	0xD1			×
Ò	0xD2			×
Ó	0xD3			×
Ô	0xD4			×
Õ	0xD5			×
Ö	0xD6			×
×	0xD7			×
Ø	0xD8			×
Ù	0xD9			×
Ú	0xDA			×
Û	0xDB			×
Ü	0xDC			×
Ý	0xDD			×
Þ	0xDE			×
ß	0xDF			×
à	0xE0			×
á	0xE1			×
â	0xE2			×
ã	0xE3			×
ä	0xE4			×
å	0xE5			×
æ	0xE6			×
ç	0xE7			×
è	0xE8			×

Zeichen	Hex	LCD	SK	PW
é	0xE9			×
ê	0xEA			×
ë	0xEB			×
ì	0xEC			×
í	0xED			×
î	0xEE			×
ï	0xEF			×
ð	0xF0			×
ñ	0xF1			×
ò	0xF2			×
ó	0xF3			×
ô	0xF4			×
õ	0xF5			×
ö	0xF6			×
÷	0xF7			×
ø	0xF8			×
ù	0xF9			×
ú	0xFA			×
û	0xFB			×
ü	0xFC			×
ý	0xFD			×
þ	0xFE			×
ÿ	0xFF			×

12 Legal

12.1 Exclusion of liability

We assume no liability for the safety of your data. The reasons for it are:

1. By choosing AES, an encryption algorithm was chosen, which meets the current standard, was tested extensively, and so far, has resisted any effort to be decrypted. However, it can not be excluded, that at any point in the future, a possibility will be found to decrypt it.

2. In addition, the safety of data very much depends on the chosen password. A careless chosen and/or too short password is easy to figure out.

12.2 PWS-Program Terms of use

With the currently available software, it is not possible to create programs in a way, that they can be operated error-free in all applications and combinations.

We would like to point out, that, despite extensive and detailed tests, there still may be system configurations, which can cause the program and possibly the processor to crash.

We assume no liability regarding malfunctions that occurred and their consequential damages. Hereunder included are also malfunctions and damages to other installed software products on your processor and the saved data.

Please, by all means, backup your data first, before installing and using the program!
When installing the Program-CD, we do assume, that the user has noticed this information.

The manual, included on the CD, expresses the basic functions of the program.

We reserve the right to change, add or remove parts of the program without prior notice. There is no obligation for a free of charge re-fitting on our part.

12.2.1 Use of the program

With the purchase of this program, only the license to use this program is purchased. The license only applies for the purchased version. Functions, exceeding the current version, will only become binding after a written acceptance was issued on our part.

The licensee is authorized, to copy the purchased program version as often as required for his own use and to use it himself. Unauthorized duplication, transfer, rental or lease to third parties, granting of sublicenses, as well as changing the manual are not allowed.

12.2.2 Warranty

We only guarantee those functions, described in the respective version of the manual. We do not guarantee, that this program will work error-free in all system configurations chosen by the user.

13 Technical Data

Dimensions: approx. 83 mm × 42 mm × 18 mm (L × W× H)

Weight: approx. 28 g (with battery)

PC-Interface: USB 1.1 or higher, via USB-UART-Bridge

Transfer rate: 9600 baud, 8N1

Battery: 3V lithium battery, type CR2032

Durability: depending on the amount of uses in mobile-mode

Data sets: max. 1 000